CheckPoint

Exam Questions 156-585

Check Point Certified Troubleshooting Expert

NEW QUESTION 1
Check Point provides tools & commands to help you to identify issues about products and applications. Which Check Point command can help you to display status and statistics information for various Check Point products and applications?

A. cpstat
B. CPstat
C. CPview
D. fwstat

Answer: A

NEW QUESTION 2
Rules within the Threat Prevention policy use the Malware database and network objects. Which directory is used for the Malware database?

A. $FWDIR/conf/install_manager_tmp/ANTIMALWARE/conf/
B. $CPDIR/conf/install_manager_lmp/ANTIMALWARE/conf/
C. $FWDlR/conf/install_firewall_imp/ANTIMALWARE/conf/
D. $FWDlR/log/install_manager_tmp/ANTIMALWARBlog?

Answer: A

NEW QUESTION 3
Which command is most useful for debugging the fwaccel module?

A. fw zdebug
B. securexl debug
C. fwaccel dbg
D. fw debug

Answer: C

NEW QUESTION 4
What does CMI stand for in relation to the Access Control Policy?

A. Content Matching Infrastructure
B. Content Management Interface
C. Context Management Infrastructure
D. Context Manipulation Interface

Answer: C

NEW QUESTION 5
What is the main SecureXL database for tracking the acceleration status of traffic?

A. cphwd_db
B. cphwd_tmp1
C. cphwd_dev_conn_table
D. cphwd_dev_identity_table

Answer: D

NEW QUESTION 6
Which of the following is a component of the Context Management Infrastructure used to collect signatures in user space from multiple sources, such as Application Control and IPS. and compiles them together into unified Pattern Matchers?

A. CMI Loader
B. cpas
C. PSL - Passive Signature Loader
D. Context Loader

Answer: A

NEW QUESTION 7
Select the technology that does the following actions
- provides reassembly via streaming for TCP
- handles packet reordering and congestion
- handles payload overlap
- provides consistent stream of data to protocol parsers

A. Passive Streaming Library
B. Context Management
C. Pre-Protocol Parser
D. fwtcpstream

Answer:

A

NEW QUESTION 8
What is NOT a benefit of the fw ctl zdebug command?

A. Cannot be used to debug additional modules
B. Collect debug messages from the kernel
C. Clean the buffer
D. Automatically allocate a 1MB buffer

Answer: A

NEW QUESTION 9
If the cpsemd process of SmartEvent has crashed or is having trouble coming up. then it usually indicates that .

A. Postgres database ts down
B. Cpd daemon is unable to connect to the log server
C. The SmartEvent core on the Solr mdexer has been deleted
D. The logged in administrator does not have permissions to run SmartEvent

Answer: C

NEW QUESTION 10
What are the main components of Check Point's Security Management architecture?

A. Management server, management database, log server, automation server
B. Management server, Security Gatewa
C. Multi-Domain Server, SmartEvent Server
D. Management Serve
E. Log Serve
F. LDAP Server, Web Server
G. Management server Log server, Gateway serve
H. Security server

Answer: A

NEW QUESTION 10
You need to run a kernel debug over a longer period of time as the problem occurs only once or twice a week. Therefore, you need to add a timestamp to the kernel debug and write the output to a file but you can't afford to fill up all the remaining disk space and you only have 10 GB free for saving the debugs. What is the correct syntax for this?

A. fw ctl kdebug -T -f -m 10 -s 1000000 -o debugfilename
B. fw ctl kdebug -T -f -m 10 -s 1000000 > debugfilename
C. fw ctl kdebug -T -m 10 -s 1000000 -o debugfilename
D. fw ctl debug -T -f -m 10 -s 1000000 -o debugfilename

Answer: D

NEW QUESTION 12
PostgreSQL is a powerful, open source relational database management system Check Point offers a command for viewing the database to interact with Postgres interactive shell Which command do you need to enter the PostgreSQL interactive shell?

A. psql_client cpm postgres
B. mysql_client cpm postgres
C. psql_c!ieni postgres cpm
D. mysql -u root

Answer: A

NEW QUESTION 16
Which command can be run in Expert mode lo verify the core dump settings?

A. grep cdm /config/db/coredump
B. grep cdm /config/db/initial
C. grep SFWDIR/config/db/initial
D. cat /etc/sysconfig/coredump/cdm conf

Answer: C

NEW QUESTION 19
You are upgrading your NOC Firewall (on a Check Point Appliance) from R77 to R80 30 but you did not touch the security policy After the upgrade you can't connect to the new R80 30 SmartConsole of the upgraded Firewall anymore What is a possible reason for this?

A. new new console port is 19009 and a access rule ts missing
B. the license became invalig and the firewall does not start anymore
C. the upgrade process changed the interfaces and IP adresses and you have to switch cables

D. the IPS System on the new R80.30 Version prohibits direct Smartconsole access to a standalone firewall

Answer: D

NEW QUESTION 21
Which file is commonly associated with troubleshooting crashes on a system such as the Security Gateway?

A. core dump
B. CPMIL dump
C. fw monitor
D. tcpdump

Answer: A

NEW QUESTION 22
Your users have some issues connecting Mobile Access VPN to the gateway. How can you debug the tunnel establishment?

A. in the file $CVPNDIR/conf/httpd.conf change the line loglevel .. To LogLevel debug and run cvpnrestart
B. run vpn debug truncon
C. run fw ctl zdebug -m sslvpn all
D. in the file $VPNDIR/conf/httpd.conf the line Loglevel .. To LogLevel debug and run vpn restart

Answer: A

NEW QUESTION 25
What is the function of the Core Dump Manager utility?

A. To generate a new core dump for analysis
B. To limit the number of core dump files per process as well as the total amount of disk space used by core files
C. To determine which process is slowing down the system
D. To send crash information to an external analyzer

Answer: B

NEW QUESTION 27
URL Filtering is an essential part of Web Security in the Gateway. For the Security Gateway to perform a URL lookup when a client makes a URL request, where is the sync-request forwarded from if a sync-request is required"

A. RAD Kernel Space
B. URLF Kernel Client
C. URLF Online Service
D. RAD User Space

Answer: B

NEW QUESTION 28
For TCP connections, when a packet arrives at the Firewall Kernel out of sequence or fragmented, which layer of IPS corrects this to allow for proper inspection?

A. Passive Streaming Library
B. Protections
C. Protocol Parsers
D. Context Management

Answer: A

NEW QUESTION 29
After kernel debug with "fw ctl debug" you received a huge amount of information It was saved in a very large file that is difficult to open and analyze with standard text editors Suggest a solution to solve this issue.

A. Use "fw ctl zdebug' because of 1024KB buffer size
B. Divide debug information into smaller files Use "fw ctl kdebug -f -o "filename" -m 25 - s "1024"
C. Reduce debug buffer to 1024KB and run debug for several times
D. Use Check Point InfoView utility to analyze debug output

Answer: C

NEW QUESTION 30
The Check Pom! Firewall Kernel is the core component of the Gaia operating system and an integral part of the traffic inspection process There are two procedures available for debugging the firewall kernel Which procedure/command is used for troubleshooting packet drops and other kernel activites while using minimal resources (1 MB buffer)?

A. fw ctl zdebug
B. fw ctl debug/kdebug
C. fwk ctl debug
D. fw debug ctl

Answer: A

NEW QUESTION 32
VPN's allow traffic to pass through the Internet securely by encrypting the traffic as it enters the VPN tunnel and then decrypting the exists. Which process is responsible for Mobile VPN connections?

A. cvpnd
B. vpnd
C. vpnk
D. fwk

Answer: C

NEW QUESTION 37
How can you increase the ring buffer size to 1024 descriptors?

A. set interface eth0 rx-ringsize 1024
B. fw ctl int rx_ringsize 1024
C. echo rx_ringsize=1024>>/etc/sysconfig/sysctl.conf
D. dbedit>modify properties firewall_properties rx_ringsize 1024

Answer: A

NEW QUESTION 38
What is the name of the VPN kernel process?

A. VPNK
B. VPND
C. CVPND
D. FWK

Answer: A

NEW QUESTION 42
Check Point Access Control Daemons contains several daemons for Software Blades and features Which Daemon is used for Application & Control URL Filtering?

A. rad
B. cprad
C. pepd
D. pdpd

Answer: C

NEW QUESTION 46
Which of the following daemons is used for Threat Extraction?

A. scrubd
B. extractd
C. tex
D. tedex

Answer: A

NEW QUESTION 49
To check the current status of hyper-threading, which command would you execute in expert mode?

A. cat /proc/hypert_status
B. cat /proc/smt_status
C. cat /proc/hypert_stat
D. cat /proc/smt_stat

Answer: B

NEW QUESTION 53
......